

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

Mark Wiedder, individually and on behalf of
themselves and all others similarly situated,

Plaintiff,

v.

Flagstar Bank, FSB, a Michigan-based
federally chartered stock savings bank;

Defendant.

Case No. _____

CLASS ACTION

JURY TRIAL DEMANDED

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Plaintiff Mark Wiedder (“Plaintiff”), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the “Action”) against the above-captioned Defendant, Flagstar Bank, FSB (hereinafter “Flagstar” or the “Defendant”), upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this Action against Defendant for its failure to properly secure and safeguard personally identifiable information that Defendant stored on

its network systems, including, without limitation, names, addresses, Social Security numbers, financial information (e.g. account numbers, credit or debit card numbers), and “other” types of information (collectively, “personally identifiable information” or “PII”). This is the second data breach of Defendant’s information data base in less than two years, resulting in the exfiltration of consumer data, and was therefore entirely foreseeable.

2. According to its website, Defendant “has assets of \$31.0 billion, is the sixth largest bank mortgage originator nationally, and the second largest savings bank in the country.” Defendant “operate[s] 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio and provide[s] a full complement of products and services for consumers and businesses.” Its “mortgage division operates nationally through 103 retail locations and a wholesale network of approximately 2,350 third-party mortgage originators.”

3. Defendant’s customers entrust Defendant with an extensive amount of their PII. Defendant retains this information on computer hardware—even after the customer relationship ends. Defendant asserts that it understands the importance of protecting such information.

4. On or before June 2, 2022, Defendant discovered that an unauthorized actor “accessed and/or acquired” the information of more than 1,500,000 individuals

from its network between December 3, 2021 and December 4, 2021 (the “Data Breach”).

5. On or before June 20, 2022, Defendant reported that the types of affected information included, without limitation, names, addresses, Social Security numbers, financial information (e.g. account/loan numbers, credit or debit card numbers), and “other” types of information required by Defendant from Plaintiff and Class Members on mortgage applications.

6. This was Defendant’s second major data breach in 2021. Indeed, on or before January 22, 2021, Defendant learned that an unauthorized actor breached Defendant’s vendor’s file sharing platform, which Defendant had used to store its current and previous customers’ information. Less than one year later, yet another unauthorized actor accessed and/or acquired PII collected, stored, and maintained by Defendant - despite Defendant’s assertions that it was taking steps to secure the PII of its customers following its previous data security incident.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class Members’ PII, Defendant assumed legal and equitable duties to those individuals.

8. Defendant’s internal systems contain millions of individuals’ detailed and highly sensitive PII. Defendant admits that the Data Breach involved unauthorized access and activity on their internal systems and that the names, or

other personal identifiers in combination with Social Security numbers of 1,547,169 individuals were affected.

9. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. It took more than six months for Defendant to publicly report this Data Breach. The compromised PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing millions of Social Security numbers.

10. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. It is unclear whether Defendant has yet provided notice of the Data Breach to all affected individuals, and Defendant still maintains as secret the specific vulnerabilities and root causes of the Data Breach. Plaintiff and Class Members also remain unaware of precisely what information was accessed and subject to unauthorized activity and for how long. Nearly six months passed before Defendant "discovered" that Plaintiff's and Class Members' PII was accessed and/or acquired by unauthorized actors – allegedly on or before June 2, 2022 – leaving Plaintiff and

Class Members exposed, without knowledge or recourse, for the entirety of that time.

11. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiff and Class Members for a second time in the span of one year.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) comply with industry standards to protect information systems that contain PII. Defendant's conduct amounts to negligence and violates federal and state statutes. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to fully and accurately disclose the circumstances under which that information was compromised, to adopt reasonably sufficient security practices and safeguards to prevent future unauthorized access, disclosure, and exfiltration, and to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members.

13. Following the breach and recognizing that Plaintiff, along with each and every Class Member, are now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members credit

monitoring and identity repair services for twenty-four months through Kroll. The offered services are insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII accessed, acquired, exfiltrated, and/or published onto the internet. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

14. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII

was safeguarded, failing to take available steps to prevent another unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to and/or acquisition by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

16. Plaintiff Mark Wiedder is a citizen of Orange County, California, who received a Data Breach notification letter from the Defendant dated June 15, 2022.

17. Defendant Flagstar Bank, FSB, is a Michigan-based federally chartered stock savings bank, headquartered at 5151 Corporate Drive, Troy, Michigan.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant to establish minimal diversity – namely, Plaintiff is a California resident whereas Defendant is headquartered in Michigan, specifically in this District.

21. The Eastern District of Michigan has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Michigan and this District through its headquarters, offices, parents, and affiliates.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

23. Defendant used its internal systems to store and/or share some of Plaintiff's and Class Members most sensitive and confidential information,

including but not limited to names, addresses, Social Security numbers, financial information (e.g. account numbers, credit or debit card numbers), and “other” types of personal identifiable information, which is static, does not change, and can be used to commit myriad financial crimes.

24. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect Plaintiff’s and Class Members’ PII from involuntary disclosure to third parties.

The Data Breach

26. On or about June 17, 2022, Defendant reported the Data Breach to the Office of the Maine Attorney General. Defendant’s report included a “Standard Notification Letter” that read, in part, as follows:

Flagstar Bank treats the security and privacy of your personal information with the utmost importance, which is why we are writing to let you know about a recent security incident. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to help protect your information.

What Happened?



Flagstar recently experienced a cyber incident that involved unauthorized access to our network. In response, Flagstar promptly

took steps to secure its environment and investigate the incident with the assistance of third-party forensic experts.

What We Are Doing.

Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. After an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that certain impacted files containing your personal information were accessed and/or acquired from our network between December 3, 2021 and December 4, 2021. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

On June 2, 2022, we determined that one or more of the impacted files contained your  .

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Please review the attachment to this letter, entitled “Steps You Can Take to Help Protect Your Information,” for further information. The attachment also includes the toll-free telephone numbers and addresses of the three major credit reporting agencies. Additionally, you should always remain vigilant in reviewing your financial account

statements and credit reports for fraudulent or irregular activity on a regular basis.

27. On or about June 17, 2022, Defendant notified other states Attorneys General of the Data Breach, including Texas and California.

28. Defendant notified the Office of the Maine Attorney General that the information of 1,547,169 individuals was accessed and/or acquired on or about December 3, 2021 through December 4, 2021, and that information included names and other personal identifiers in combination with Social Security numbers.

29. On or about June 20, 2022, Defendant notified the Attorney General of Texas that the affected types of PII included: name of individual; address; Social Security Number information; financial information (e.g. account number, credit or debit card number); and “other” types of information.

30. Defendant admitted in the Notice of Data Breach, the reports to the Attorneys General, and the “sample” notices of the Data Breach that an unauthorized party accessed and/or acquired one or more documents that contained sensitive information about Defendant’s current and former customers, including names, addresses, Social Security numbers, financial information (e.g. account numbers, credit or debit card numbers), and “other” types of personal identifiable information.

31. In response to the Data Breach, Defendant claims that it “promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal

law enforcement.” However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected. Learning of this information is especially important considering this was Defendant’s second data breach in less than one year.

32. Plaintiff’s and Class Members’ unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII to be exposed.

Defendant Acquires, Collects, and Stores Plaintiff’s and Class Members’ PII

34. Defendant has a posted privacy policy (“Privacy Policy”)¹⁴ on its website, at the bottom of its homepage, under a tab entitled “Security.” The Privacy Policy was last revised in February of 2018. The Privacy Policy states “[f]inancial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to

tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.”

35. The types of personal information Defendant collects, and potentially shares, “depend[s] on the product or service” customers have with Defendant.

36. Defendant states it collects PII, among other types of information, including: “Social Security number and credit scores[;] Account transactions and checking account information[; and] Transaction history and payment history.”

37. Defendant states that it continues to retain this PII and other sensitive information for former customers, and that it “continue[s] to share your information as described in this notice.”

38. Defendant states that “All financial companies need to share customers’ personal information to run their everyday business.” Defendant then lists permissible purposes that it may share customers’ information, none of which are applicable here.

39. Defendant acquired, collected, and stored Plaintiff’s and Class Members’ PII.

40. As a condition of providing services to its customers, Defendant requires that its customers entrust Defendant with highly confidential PII.

41. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

43. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former customers.

44. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

45. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is further exacerbated by the data breach it experienced in January of 2021.

46. Despite the Defendant's recent previous data breach and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

47. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”

48. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of PII

49. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200. Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web. Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

51. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number,

so all of that old bad information is quickly inherited into the new Social Security number.”

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”

55. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

56. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

57. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

58. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

59. Plaintiff and Class Members are each now subject to the present and continuing risk of identity theft and fraud and now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s file servers, amounting to more than one and half million individuals’ detailed, personal information and, thus, the

significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. Following the breach and recognizing that Plaintiff, along with each and every Class Member, is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members twenty- four months of identity monitoring services through a single provider, Kroll. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

62. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.

63. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'" Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring

their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves. Defendant states its affected current and former customers to “should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.”

64. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seeks remuneration for the loss of valuable time as another element of damages.

65. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendant Violated the Gramm-Leach-Bliley Act

66. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

67. The GLBA defines a financial institution as “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956].” 15 U.S.C. § 6809(3)(A).

68. Defendant collects nonpublic personal information, as defined by 15 U.S.C.

§ 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

69. The GLBA Privacy Rule became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

70. Accordingly, Defendant’s conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

71. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy

policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

72. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers’ PII and storing that PII on Defendant’s network systems.

73. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers’ PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

74. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable

administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

75. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

76. Defendant failed to adequately evaluate and adjust its information security program in light of the previous data breach, changes to its business operation, and other relevant circumstances, including the heightened cyber-attack risk environment.

77. Further, Defendant stated that, though the Data Breach began in or around December 3, 2021, it did not “discover” the information had been accessed and/or acquired by an unauthorized third-party until June 2, 2022.

78. As of January 4, 2019, Defendant’s “Policies and Procedures” for “Compliance” recognized that the GLBA “prohibits financial institutions from sharing the non-public personal information of consumers with non-affiliated third parties except in certain circumstances.”

79. As of January 4, 2019, Defendant further recognized the GLBA required it to (a) “[p]rovide an opt-out notice prior to sharing non-public personal information with non-affiliated third parties” and (b) “[p]rovide customers with a ‘reasonable opportunity’ to opt out before disclosing non-public personal information about them to non-affiliated third parties.”

80. As of January 4, 2019, Defendant admitted that it had not provided Plaintiff or Class Members an opt-out notice, stating it “does not currently share non-public personal information with non-affiliated third parties; therefore, it is not required to and does not provide an opt-out notice.”

81. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

82. Defendant has not informed Plaintiff and Class Members of the reason Defendant kept the PII of more than 1.5 million individuals on an unsecured platform, accessible from the internet, especially considering its recent breach reported in March of 2021; if this was done to share the PII with yet another non-affiliated third party, Defendant would be further in breach of the GLBA and its own policy and procedures in failing to provide Plaintiff and Class Members an opt-out notice and a reasonable opportunity to opt out of such disclosure.

Plaintiff's Experience

83. In approximately 2011, Plaintiff Wiedder refinanced his residential mortgage loan using Defendant's services. In connection with his loan application, Mr. Wiedder provided financial and other highly sensitive information to Defendant, including his Social Security number and financial information.

84. On or about June 15, 2022, Plaintiff Wiedder learned of the Data Breach via a notice from Defendant that informed Plaintiff Wiedder that his name, account/loan number, and Social Security number had been compromised.

85. As a result of learning of the Data Breach, Plaintiff Wiedder spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, further monitoring his identity theft protections services, exploring additional credit monitoring and identity theft

insurance options, self-monitoring his financial accounts, and monitoring all services on a regular basis. This time has been lost forever and cannot be recaptured.

86. Additionally, Plaintiff Wiedder is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

87. Plaintiff Wiedder stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

88. Plaintiff Wiedder suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff Wedder entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

89. Plaintiff Wiedder suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

90. Plaintiff Wiedder has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name being placed in the hands of unauthorized third-parties and possibly criminals.

91. Plaintiff Wiedder has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

92. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

93. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class. All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Flagstar Bank on or about June 17, 2022 (the "Nationwide Class").

94. The California Sub-Class that Plaintiff seeks to represent is defined as follows:

California Class. All individuals residing in California whose PII whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Flagstar Bank on or about June 17, 2022 (the "California Class").

(Collectively, these classes are discussed in this Complaint as the "Class" or "Classes")

95. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who

make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

96. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

97. **Numerosity, Fed R. Civ. P. 23(a)(1):** The Nationwide Class (the “Class”) is so numerous that joinder of all members is impracticable. Defendant reported to the Attorney General of Maine that more than 1.5 million individuals were affected by the Data Breach.

98. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

99. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

100. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

101. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

102. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3):** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

103. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs

of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

104. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

105. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

106. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

107. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

108. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,
- i. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE (ON BEHALF OF BOTH CLASSES)

109. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

110. As a condition of being customers of Defendant, Defendant's current and former customers were obligated to provide Defendant with certain PII, including their names, Social Security numbers, home addresses, phone numbers, and dates of birth.

111. Plaintiff and the Classes entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

112. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Classes could and would suffer if the PII were wrongfully disclosed.

113. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Classes involved an unreasonable risk of harm to Plaintiff and the Classes, even if the harm occurred through the criminal acts of a third party.

114. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

115. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

116. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Classes.

117. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the

Classes. That special relationship arose because Plaintiff and the Classes entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

118. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiff or the Classes.

119. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Classes was reasonably foreseeable, particularly in light of Defendant’s inadequate security practices.

120. Plaintiff and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Classes, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant’s systems.

121. Defendant’s own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant’s misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant’s misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant and failing to delete PII it no longer had a reasonable business need to maintain.

122. Plaintiff and the Classes had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

123. Defendant was in a position to protect against the harm suffered by Plaintiff and the Classes as a result of the Data Breach.

124. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

125. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Classes.

126. Defendant has admitted that the PII of Plaintiff and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

127. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Classes during the time the PII was within Defendant's possession or control.

128. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

129. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Classes in the face of increased risk of theft.

130. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

131. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

132. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Classes the existence and scope of the Data Breach.

133. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Classes would not have been compromised.

134. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Classes and the

harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Classes was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

135. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

136. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Classes.

137. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

138. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a

comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

139. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to adequately (i) test and/or monitor the system where the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment, and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of more than 1.5 million individuals with one or more non-affiliated third parties.

140. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence per se.

141. Plaintiff and the Classes are within the class of persons that the FTC Act and the GLBA were intended to protect.

142. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

143. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII

of Plaintiff and the Classes; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Classes.

144. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

145. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF BOTH CLASSES)

146. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

147. Defendant required Plaintiff and the Classes to provide their personal information, including names, Social Security numbers, addresses, financial

information, and other personal information, as a condition of being customers of Defendant.

148. As a condition of being customers of Defendant, Plaintiff and the Classes provided their personal and financial information. In so doing, Plaintiff and the Classes entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Classes if their data had been breached and compromised or stolen.

149. Plaintiff and the Classes fully performed their obligations under the implied contracts with Defendant.

150. Defendant breached the implied contracts it made with Plaintiff and the Classes by failing to safeguard and protect their personal and financial information, including by failing to implement basic encryption techniques freely available to Defendant and failing to delete PII it no longer had a reasonable business need to maintain, and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

151. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Classes have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes,

fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
(ON BEHALF OF BOTH CLASSES)

152. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

153. Plaintiff and the Classes had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

154. Defendant owed a duty to its current and former customers, including Plaintiff and the Classes, to keep their PII contained as a part thereof, confidential.

155. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Classes.

156. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Classes, by way of Defendant's failure to protect the PII.

157. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Classes is highly offensive to a reasonable person.

158. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Classes is of no legitimate concern to the public.

159. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Classes disclosed their PII to Defendant as part of the current and former customers' relationship with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Classes were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

160. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Classes' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

161. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

162. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

163. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Classes was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

164. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Classes have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

165. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Classes are entitled to recover actual, consequential, and nominal damages.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(ON BEHALF OF BOTH CLASSES)

166. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

167. At all times during Plaintiff's and the Classes' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Classes' PII that Plaintiff and the Classes provided to Defendant.

168. As alleged herein and above, Defendant's relationship with Plaintiff and the Classes was governed by terms and expectations that Plaintiff's and the Classes' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

169. Plaintiff and the Classes provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

170. Plaintiff and the Classes also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

171. Defendant voluntarily received in confidence the PII of Plaintiff and the Classes with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

172. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Classes was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Classes' confidence, and without their express permission.

173. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Classes have suffered damages.

174. But for Defendant's disclosure of Plaintiff's and the Classes' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Classes' PII as well as the resulting damages.

175. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Classes' PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Classes' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Classes' PII.

176. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Classes, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Classes.

177. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
(ON BEHALF OF THE CALIFORNIA CLASS)

178. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

179. Defendant's unlawful business acts and practices as complained of herein violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (the "UCL").

180. Specifically, Defendant engaged in unlawful business acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting and gathering the PII of Plaintiff and the California Class knowing that the information would not be adequately protected, and by storing the PII of Plaintiff and the California Class in an unsecure electronic system, all in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to undertake reasonable measures to safeguard the PII of Plaintiff and the California Class, as well as the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule.

181. Defendant knew or should have known that its data security practices with respect to its computer systems were inadequate to safeguard the PII of Plaintiff and the California Class and that, as a result, the risk of a data breach or theft was highly likely. Defendant's unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the California Class.

182. As a direct and proximate result of Defendant's unlawful business acts and practices, Plaintiff and the California Class suffered injury in fact and lost money

or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

183. In addition, Plaintiff and the California Class have incurred and will continue to incur economic damages related to the Data Breach, including loss of time and money spent remedying the Data Breach, and the costs of credit monitoring, purchasing credit reports, and implementing credit freezes to prevent opening of unauthorized account, among others.

184. Specifically, Defendant engaged in unfair business acts and practices by failing to establish adequate security practices and procedures, by soliciting and collecting the PII of Plaintiff and the California Class, knowing that the information would not be adequately protected, and by storing the PII in an unsecure electronic system. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or damaging to Plaintiff and the California Class as they were likely to deceive them into believing their PII was securely stored when it was not.

185. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the California Class outweighs the utility of Defendant's conduct. This conduct includes Defendant's failure to adequately ensure the privacy,

confidentiality, and security of the data Plaintiff and the California Class entrusted to them and Defendant's failure to have adequate data security measures in place.

186. Specifically, Defendant engaged in unfair acts and practices by failing to enact adequate privacy and security measures and protect the PII of Plaintiff and the California Class from unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and damaging to Plaintiff and the California Class.

187. As a direct and proximate result of Defendant's unfair business practices and acts, Plaintiff and the California Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

188. Accordingly, Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or property that Defendant acquired by means of its unlawful and unfair business acts and practices, disgorgement of all profits Defendant received as a result of its unlawful business practices, declaratory relief, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and injunctive or other equitable relief.

VII. PRAYER FOR RELIEF

189. WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Nationwide Class and the California Class and appointing Plaintiff and his Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - b. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - c. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless

Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- e. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- f. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- g. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- h. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

- i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- j. requiring Defendant to conduct regular database scanning and securing checks;
- k. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- l. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- m. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and

periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- n. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- o. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- p. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report

to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands that this trial be tried before a jury.

Dated: June 28, 2022

/s/ Nick Suciu, III

Nick Suciu III (P72052)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Phone: 313-303-3742
Email: nsuciu@milberg.com

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866-252-0878
Email: gklinger@milberg.com

M. Anderson Berry
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 239-4778
Email: aberry@justice4you.com